ABSTRACT

In a postage meter system, a user enters information indicative of a batch of mail pieces to be franked. The mail pieces are franked, and when the batch is completed, data relating to the batch are made the subject of a cryptographic engine. The data are digitally signed, or a message authentication code (MAC) is derived, all in a postal security device (PSD). The data are communicated to a server, where the data are authenticated, preferably by means of public-key cryptographic means. These data are then made available to the postal authority in a secure way.

Customer accounting is based on statistical data gathered by the postage printing base. Such data may be accumulated and stored in the PSD or in the postage printing base outside of the PSD. The cryptographic protection inherent in the PSD, of the sensitive data, effectively detects or prevents tampering. In addition effective backup and recovery mechanisms may be put into place to protect customer as well as third-party interests. In order to assure the authenticity and accuracy of the data collected, the use of a PSD solves both the guarantee of authenticity and accuracy of the data collected for use by the postal authority. Using the data collected by the PSD as input for the calculation of the discount allows for payback calculations due the customers (or allows for giving customers credit for future services).